IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	William J. Eakin	Examiner: Stephen D'Agosta
Serial No.:	10/685,366	Group Art Unit: 2617
Filed:	October 14, 2003	Docket No.: 10018596-1
Title:	System and Method for Remotely Accessing a Private Database	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is filed in response to the Final Office Action mailed May 8, 2006 and the Notice of Appeal filed on August 8, 2006.

AUTHORIZATION TO DEBIT ACCOUNT

It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's deposit account no. 08-2025.

I. REAL PARTY IN INTEREST

The real party-in-interest is the assignee, Hewlett-Packard Development Company, L.P., a Texas Limited Partnership having its principal place of business in Houston, Texas.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences known to appellant, the appellant's legal representative, or assignee that will directly affect or be directly affected by or have a bearing on the Appeal Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 – 32 stand finally rejected. The rejection of claims 1 – 32 is appealed.

IV. STATUS OF AMENDMENTS

In the Final Office Action mailed May 8, 2006, claim 1 was rejected under 35 USC § 112, second paragraph, as having insufficient antecedent basis for the term "application ID." Applicant filed an After Final Response under 37 CFR 1.116 to correct this typographical error in claim 1. Specifically, claim 1 was amended as follows: the appliance ~~application~~ ID. The Examiner entered this amendment. Thus, all amendments have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element or that these are the sole sources in the specification supporting the claim features.

Embodiments of the invention, such as embodied in claim 1 comprises:

A method for communicating information from a private database (FIG. 2: #218) to a wireless communication device (FIG. 2: #100), the method comprising (FIG. 4; para. [44]: p. 11, lines 10-31):

receiving a private database access request from the wireless communication device, the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device (FIG. 4: #404; para. [45]: p. 11, line 32 – p. 12, line 6);

comparing the appliance ID with a security indicia, the security indicia associated with the wireless communication device (FIG. 4: #406; para. [45]: p. 11, line 32 – p. 12, line 6); and

communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia, wherein verification of only the appliance ID is sufficient to authorize access to the private database (FIG. 4: #408; para. [45]: p. 11, line 32 – p. 12, line 6; para; [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 12 comprises:

A method for remotely accessing a private database (FIG. 2: #218) residing in a remote database device (FIG. 2: #126) using a wireless communication device (FIG. 2: #100), the method comprising (FIG. 3: para. [42]: p. 10, lines 12-32):

transmitting a radio frequency (RF) communication to the remote database device, the RF communication comprising a private database access request and comprising an appliance identification (ID) that uniquely identifies the wireless communication device (FIG. 3: #304; para. [43]: p. 11, lines 1-9); and

verifying only the appliance ID in order to authorize the wireless communication device to access the private database (para [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 14 comprises:

The method of claim 12, further comprising transmitting a phone number of the wireless communication device as the appliance ID (para. [34]: p.8, lines 6-19, [36]: p. 8, lines 25-33).

An embodiment of the invention such as embodied in claim 15 comprises:

The method of claim 12, further comprising accessing the private database based on identification and authorization of the wireless communication device, not identification of a user of the wireless communication device (para. [16]: p. 3, lines 21-30, [34-36]: p.8, lines 6 - 33).

Embodiments of the invention, such as embodied in claim 16 comprises:

The method of claim 12, further comprising granting access to the private database without requiring a user of the wireless communication device to enter a password (para. [36]: p. 8, lines 25-33).

Embodiments of the invention, such as embodied in claim 19 comprises:

A system (FIG. 1: #100) that remotely accesses a private database (FIG. 2: #218) using a wireless communication device (FIG. 2: #100), the wireless communication device comprising (FIGS. 1 and 2: para. [16]: p. 3, lines 21-30, [18]: p. 4, lines 8-14):

a transceiver (FIG. 2: #216) configured to receive and transmit radio frequency (RF) communications; (para. [19]: p. 4, lines 14-21, [25]: p. 5, line 31 – p. 6, line 9)

an appliance identification (ID) (FIG. 2: #210) corresponding to a multiple-use unique identifier of the wireless communication device (FIG. 2: #100) that is included in all transmitted RF communications from the wireless communication device (para. [28]: p. 6, line 24 – p. 7, line 2); and

a processor (FIG. 2: #202) configured to cause the transceiver to transmit a first RF communication to a database device (FIG. 1: #126) having at least one private database (FIG. 2: #218), the first RF communication comprising the appliance ID and a private database access request so that verification of only the appliance ID authorizes the wireless communication device to access information stored in the private database (para.

[23-28]; FIG. 3: #304, 306; para. [42-43]: p. 10, line 12 – p.11, line 9; para [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 22 comprises:

A system (FIG. 1: #100) that provides accesses to a private database (FIG. 2: #218) comprising: (FIGS. 1 and 2; para. [16]: p. 3, lines 21-30, [18]: p. 4, lines 8-13)

a communication system interface (FIG. 2: #224) configured to receive a private database access request and a multiple-use unique identifier (ID) generated by a remote wireless communication device (FIG. 2: #100) and configured to transmit a private database (FIG. 2: #218) to the remote wireless communication device (para. [28-29]: p. 6, line 24 – p. 7, line 13; FIG. 4: #404; para. [44-45]: p. 11, line 10 – p.12, line 6);

a security indicia (FIG. 2: #234) that corresponds to the multiple-use unique ID, the multiple-use unique ID being included in all communications from the wireless communication device and uniquely identifying the wireless communication device (para. [28]:p. 6, line 24 – p. 7, line 2, [33]: p. 7, line 27 – p. 8, line 5); and

a processor (FIG. 2: #226) configured to compare the multiple-use unique ID to the security indicia, and further configured to cause communication of the private database to the remote wireless communication device when the multiple-use unique ID corresponds to the security indicia, wherein verification of only the multiple-use unique ID is sufficient to authorize access to the private database (para. [29-30]: p. 7, lines 13-18, [33]; FIG. 4: #406; para. [45]: p. 11, line 32 – p. 12, line 6; para [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 24 comprises:

A computer-readable medium having a program for remotely accessing remote private databases (FIG. 2: #218) using a wireless communication device (FIG. 2: #100), the program comprising logic configured to (FIG. 3: para. [42]: p. 10, lines 12-32, [57]: p. 16, lines 1-6):

cause a transceiver to transmit a first radio frequency (RF) communication comprising a private database access request and a multiple-use unique identifier that uniquely identifies the wireless communication device, the first RF communication

directed to a remote database device wherein a private database resides, and wherein the multiple-use unique identifier is included in all RF communications from the wireless communication device (FIG. 3: #304; para. [28]: p. 6, line 24 – p. 7, line 2, [43]: p. 11, lines 1-9); and

cause the transceiver to receive a second RF communication comprising at least the private database, the private database communicated to the wireless communication device by the remote database device when the multiple-use unique identifier corresponds to a security number residing in the remote database device, wherein verification of the multiple-use unique identification alone is sufficient to authorize access to the private database (FIG. 3: #306; para. [43]: p. 11, lines 1-9; para [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 25 comprises:

A method for communicating information from a private database (FIG. 2: #218) to a wireless telephone (FIG. 2: #100), the method comprising (FIGS. 3 and 4: para. [42]: p. 10, lines 12-32, [44]: p. 11, lines 10-31):

transmitting a radio frequency (RF) communication from the wireless telephone to a remote database device wherein the private database resides, the RF communication comprising at least a private database access request and comprising an appliance identification (ID) that uniquely identifies the wireless telephone, the appliance ID being included in all communications from the wireless telephone and uniquely identifying the wireless telephone (FIG. 3: #304; para. [43]: p. 11, lines 1-9);

receiving the private database access request and the appliance ID by the remote database device (FIG. 4: #404; para. [45]: p. 11, line 32 – p. 12, line 6);

comparing only the appliance ID with a security indicia to determine if the wireless telephone has authorization to access the private database, the security indicia associated with the wireless communication device (FIG. 4: #406; para. [45]: p. 11, line 32 – p. 12, line 6; para [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18);

communicating the information of the private database from the remote database device when the appliance ID corresponds to the security indicia (FIG. 4: #408; para. [45]: p. 11, line 32 – p. 12, line 6); and

receiving a second RF communication by the wireless telephone comprising at least the information of the private database (FIG. 3: #306; para. [43]: p. 11, lines 1-9).

Embodiments of the invention, such as embodied in claim 27 comprises:

A method of software execution for remotely accessing a remote database (FIG. 2: #126) using a portable wireless communication device (PWCD) (FIG. 2: #100), the method comprising (FIGS. 3 and 4; para. [42]: p. 10, lines 12-32, [44]: p. 11, lines 10-31):

transmitting, via a radio frequency (RF) communication, an access request from the PWCD to the remote database, the access request including an identification of the remote database and an identification (ID) of the PWCD (FIG. 3: #304; para. [43]: p. 11, lines 1-9);

receiving, via an internet, the access request at the remote database (FIG. 4: #404; para. [45]: p. 11, line 32 – p. 12, line 6, [21]: p. 5, lines 1-12); and

verifying, at the remote database, only the ID to determine whether the PWCD has authority to access information stored in the remote database (FIG. 4: #406; para. [45]: p. 11, line 32 – p. 12, line 6; para; [16]: p. 3, lines 21-30, [29]: p. 7, lines 3-13, [30]: p. 7, lines 14-18).

Embodiments of the invention, such as embodied in claim 28 comprises:

The method of claim 27 further comprising transmitting, via both the internet and the RF communication, the information from the remote database to the PWCD (FIG. 1: para. [19-22]: p. 4, line 14 – p. 5, line 17).

Embodiments of the invention, such as embodied in claim 30 comprises:

The method of claim 27 wherein the PWCD is a cellular phone, and the ID is a cellular phone number of the cellular phone (para. [34]: p.8, lines 6-19).

Embodiments of the invention, such as embodied in claim 31 comprises:

The method of claim 27 further comprising recognizing, at the remote database, a cellular phone number in the access request for identifying the PWCD as authorized to access the information stored in the remote database (para. [34]: p.8, lines 6-19, [36]: p. 8, lines 25-33, [45]: p. 11, line 32 – p. 12, line 6).

Embodiments of the invention, such as embodied in claim 32 comprises:

The method of claim 27 further comprising authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in the remote database (para. [16]: p. 3, lines 21-30, [36]: p. 8, lines 25-33).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claim 1 is rejected under 35 USC § 112, second paragraph, as failing to particularly point and distinctly claim the subject which applicant regards as his invention.

II. Claims 1 – 31 are rejected under 35 USC § 103 as being unpatentable over US 2002/0069355 (Garrison) in view of US 2002/0077077 (Rezvani) and (Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki).

III. Claim 32 is rejected under 35 USC § 103 as being unpatentable over Garrison and Rezvani and (Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki) in further view of USPN 6,178,505 (Schneider).

VII. ARGUMENT

The rejections of claims 1 – 32 are improper, and Applicant respectfully requests withdrawal of these rejections.

The claims do not stand or fall together. Instead, Applicant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

I. Claim Rejections: 35 USC § 112, Second Paragraph

Claim 1 is rejected under 35 USC § 112, second paragraph, as failing to particularly point and distinctly claim the subject which applicant regards as his invention. This rejection is moot. Specifically, Applicant filed an After Final Response under 37 CFR 1.116 to correct this typographical error. Claim 1 was amended as follows: the appliance ~~application~~ ID. The Examiner entered this amendment.

II. Claim Rejections: 35 USC § 103(a)

Claims 1 – 31 are rejected under 35 USC § 103 as being unpatentable over US 2002/0069355 (Garrison) in view of US 2002/0077077 (Rezvani) and (Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki). This rejection is traversed.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art cited must teach or suggest all the claim limitations. *See* M.P.E.P. § 2143. For at least the following reasons, these criteria have not been met, and the Office Action has failed to establish a prima facie case of obviousness.

Overview of Garrison & Rezvani

As a precursor to the arguments, Applicant provides an overview of Garrison and Rezvani.

Garrison discusses systems and methods for enabling a user or client to securely access a database from a remote location (paragraph [0013]). The important aspect in Garrison is: What steps are necessary for a client to securely access the remote database? FIG. 4A in Garrison shows the numerous steps involved for a client to securely access the remote database. Generally, Garrison discusses an encrypted key exchange between the client computer and the server computer. After the client registers with the server, the client and server exchange various encrypted public keys, passwords, log names, etc. in order to ensure a secure communication between the client and server (see paragraph [0064-0067]). Hackers cannot easily access the database since the client and server use a new encryption key exchange for each data session (paragraph [0043]).

Rezvani discusses systems and methods for registering and authenticating wireless devices (see Abstract and Claims). FIG. 1 of Rezvani shows a system 110 having a wireless device 210 and one or more controllers 28 (such as sensors, appliances, VCRs, microwave ovens, or thermostats: see paragraph [0037]). The controller has a discovery mode and an operation mode. In the discovery mode, the controller registers the wireless device; and in the operation mode, the controller receives data from the wireless device (Abstract). In the discovery mode, the wireless device transmits registration data to the controller to enable the controller to interface with the wireless device (Abstract and paragraph [0012]).

No Suggestion/Motivation to Modify/Combine References

For at least the following reasons, no suggestion or motivation exists to modify or combine Garrison in view of Rezvani.

First, Applicant argues that no teaching or suggestion exists to make the combination because the references are directed to completely different art and completely unrelated inventions. Garrison is directed to establishing a secure connection between a client computer and a server computer so the client can safely and securely access a database (see [0014]). In Garrison, a new encryption key is used for each new

data session to inhibit unauthorized users (i.e., hackers) from accessing the database (see [0042]). By contrast, Rezvani is directed to automatically detecting a wireless device and registering the wireless device with a controller (see [0055], Abstract, and Summary).

The Examiner must provide *objective evidence*, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Such teaching or suggestion does not exist.

Second, Applicant notes that no teaching or suggestion exists to make the combination because the references are directed to solving completely different problems. In Garrison, the Background section discusses security concerns because unauthorized remote users can hack into databases. In fact, Garrison explicitly provides a "need paragraph" and states that a need exists "for providing a more secure system and method of allowing remote access to a database system" ([0012]). By contrast, Rezvani solves a completely different problem. In Revzani, the Background section discusses the problems with tracking wireless devices and the problems of clock drift between controllers and transmitters. Rezvani explicitly provides a "need paragraph" and states a need exists "to have a system in which the registration of the transmitter devices is flexible and sufficiently easy to perform by a user …" ([0007]).

To establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985). In light of the completely unrelated inventions and problems being solved in Garrison and Rezvani, no suggestion or motivation exists to combine or modify these references.

For at least these reasons, Applicant respectfully asks the Board of Appeals to withdraw the rejection since a *prima facie* case of obvious has not been established.

Hindsight Construction

Applicant observes that the Examiner is performing an improper piecemeal construction that uses hindsight to arrive at the claim elements. In other words, the Examiner is picking and choosing sentences or teachings from Garrison and Rezvani with hindsight of Applicant's invention to allegedly obviate the pending claims. One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988).

No Reasonable Expectation of Success

No reasonable expectation of success has been established for modifying Garrison with the teachings of Rezvani to arrive at the recitations of the claims. In other words, even assuming *arguendo* that Garrison and Rezvani are combinable (which they are not), the combination will not yield a reasonable expectation of success.

Garrison expressly teaches that a user engages numerous steps to secure a communication with a server in order to access a database. The method in Garrison is shown in FIG. 4A: the user contacts the server, the server returns an encryption key, the user supplies a password to the server, the server translates the password, the user encrypts and sends data request, etc. (see specification beginning at [0064]). In direct contrast to Garrison, Rezvani teaches embodiments that "**automatically** detect a wireless control device and register that device with the receiver/controller" (emphasis added: see [0055]). In other words, Rezvani teaches methods for automatically discovering and registering wireless devices, "such as sensors, appliances, VCRs, microwave ovens, and thermostats" (see [0037]). Garrison teaches numerous steps for a user to manually perform secure communication between a computer system and server.

In view of these deficiencies, the Office Action has failed to establish a reasonable expectation of success with a combination or modification of Garrison and Rezvani. Therefore, the *prima facie* case of obviousness has not been established.

All Elements Not Taught or Suggested

All of the elements of the claims are not taught or suggested in Garrison and Rezvani and (Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki). In other words, even assuming *arguendo* that Garrison and Rezvani are successfully combinable (which they are not), the alleged combination fails to teach or suggest all the elements in the claims. Examples for various independent and dependent claim groups are provided below.

Independent Claims 1, 12, 19, 22, 24, 25, 27

The independent claims recite numerous recitations that are not taught or suggested in the art of record. By way of example, Applicant presents arguments with regard to independent claim 1.

Claim 1 recites "wherein verification of only the application ID is sufficient to authorize access to the private database." Garrison and Rezvani do not teach or suggest at least this element. Garrison appears to teach a complex key exchange between the user and server in order to identify a user and grant access. FIG. 4A is a flow chart illustrating the method of Garrison. The client computer and server utilize a public key exchange to establish a new encryption key (see [0065]). Garrison then states how the access request is performed:

> After receiving the new encryption key from the server 17a, the client 14 encrypts the user's password and log name with the new encryption key and transmits the password and log name to the server 17a ….
>
> The server 17a compares the log name transmitted by the client 14 with the log name in the password data table entry corresponding with the password. If the log names match, the user of the client 14 is determined to be an authorized user. (See [0066 – 0067]: portions omitted for brevity).

Nowhere does this section or any section of Garrison teach or suggest that verification of only the application ID is sufficient to authorize access to the private database.

Rezvani also does not teach or suggest all the elements of independent claim 1. Paragraph [0004] of Rezvani appears to teach that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Paragraphs [0108-0111] of Rezvani state that various communication links can be used to connect a wireless device with a server. Finally, paragraph [0113] of Rezvani states that the wireless device can be various embodiments, such as cellular phones, personal digital assistants, and computers. Notice, however, that nowhere does Rezvani teach or suggest whatsoever that the ESN itself is used to provide access to a private database. In other words, Rezvani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggests that only the ESN is sufficient to authorize access to a private database.

Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki fail to cure the deficiencies of Garrison and Rezvani.

For at least these reasons, the independent claims and the dependent claims are allowable over the art of record.

Response to Office Action Arguments

The Office Action cites paragraphs 2-7, 12, 16, and 18 in Rezvani and argues that Rezvani discloses accessing remote systems by only the device ID/serial number (see FOA at p.2 and p.4). Applicant respectfully disagrees.

Paragraph [0004] of Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Rezvani also states that the wireless device can be various embodiments, such as cellular phones, personal digital assistants, and computers (see paragraph [0113]). Nowhere, however, does Rezvani teach or suggest whatsoever that the ESN itself is used to identify the wireless device and provide access to a private database. In other words, Rezvani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggests that only the ESN is sufficient to authorize access to a private database.

Independent Claims 1 and 12

Independent claims 1 and 12 and their dependent claims recite numerous limitations that are not taught or suggested in Garrison in view of Rezvani. Claim 1 is selected for discussion.

Claim 1 recites that a wireless communication device provides an access request to a private database. The access request includes "an appliance identification (ID) that uniquely identifies the wireless communication device." Nowhere does Garrison teach or suggest that the **access request itself** includes an appliance identification that uniquely identifies the wireless communication device. By contrast, Garrison teaches that the user or client transmits a password to identify himself (i.e., the user), not the appliance device. Garrison states:

> In accordance with another feature of the present invention, the client initially transmits a password to the server in order **to identify the user** of the client as an authorized user. (Emphasis added: [0016]).

In other words, Garrison teaches that the user sends a password to identify himself as an authorized user. This teaching is in contrast to the claimed recitations. Claim 1 recites receiving an access request from the wireless communication device. The access request includes an **appliance** identification (not user identification). This appliance identification "uniquely identifies the wireless communication device" (not uniquely identifies the user).

Garrison repeatedly reiterates that his access request identifies the user, not the wireless device. FIG. 4A is a flow chart illustrating the method of Garrison. The client computer and server utilize a public key exchange to establish a new encryption key (see [0065]). Garrison then teaches how the access request is performed:

> After receiving the new encryption key from the server 17a, the client 14 encrypts the user's password and log name with the new

> encryption key and transmits the password and log name to the server 17a ….
>
> The server 17a compares the log name transmitted by the client 14 with the log name in the password data table entry corresponding with the password. If the log names match, the user of the client 14 is determined to be an authorized user. (See [0066 – 0067]: portions omitted for brevity).

Nowhere does this section or any section of Garrison teach or suggest that the access request includes an appliance identification. Instead, Garrison expressly teaches that the user sends a password and log name. A password and log name, however, do not include an appliance identification. In Garrison, nowhere is the actual appliance identified and sent to the database.

For at least these reasons, claims 1 and 12 allowable over Garrison in view of Rezvani. Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki fail to cure the deficiencies of Garrison and Rezvani. A dependent claim inherits the limitations of a base claim. Thus, for at least the reasons given in connection with claims 1 and 12, the dependent claims are also allowable over the art of record.

Garrison Teaches Away

Garrison actually teaches away from the recitations of claim 1.[1] In claim 1, the database receives an access request from the wireless device. The access request includes (1) the database access request and (2) the appliance ID. If the appliance ID corresponds with security indicia, then the database allows access. In other words, access to the database depends on the appliance ID of the wireless device itself (not passwords from users). Applicant's specification supports this "simplified, yet secure, access to a private database" ([16]):

[1] Garrison also teaches away from the combination of Rezvani which teaches automatically identifying the wireless communication device.

> Accordingly, the user requesting private database access with the wireless communication device need not enter a special password or the like because the wireless communication device is recognized by the remote database device. (para. [16]).

By contrast, access to the database in Garrison depends on a complex encrypted **password key exchange** between a user and the server. Garrison expressly teaches that a user engages numerous steps exchanging various encrypted public keys, passwords, log names, etc. in order to ensure a secure communication between the client and server (see [0064-0067]).

For at least these additional reasons, claims 1 and 12 allowable over Garrison in view of Rezvani. Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki fail to cure the deficiencies of Garrison and Rezvani. A dependent claim inherits the limitations of a base claim. Thus, for at least the reasons given in connection with claims 1 and 12, the dependent claims are also allowable over Garrison in view of Rezvani.

Independent Claims 19, 22, 24, and 25

Independent claims 19, 22, 24, and 25 and their dependent claims recite numerous limitations that are not taught or suggested in Garrison in view of Rezvani. Claim 19 is selected for discussion.

Claim 19 recites a wireless communication device that comprises an **appliance** ID corresponding to a **multiple-use unique identifier** that is included in **all** transmitted RF communications from the wireless communication device. Nowhere does Garrison in view of Rezvani teach or suggest that the wireless device has an appliance ID that corresponds to a multiple-use unique identifier that is included in all transmitted RF communications.

First, Applicant argues that Garrison and Revzani do not teach or suggest that an **appliance** ID is transmitted from the wireless device to the private database in order to determine if the wireless device has access to the private database. Applicant reiterates the arguments given above in connection with claim 1: Garrison teaches that a user enters into a encrypted key exchange with a server and enters a password and log name using

encrypted keys to identify himself (i.e., the user). Nowhere does Garrison and Rezvani teach or suggest transmitting an appliance ID in all RF communications to provide a wireless device with access to a remote private database.

For at least these reasons, claims 19, 22, 24, and 25 and their dependent claims are allowable over Garrison in view of Rezvani and Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki.

Second, Applicant respectfully cites MPEP §2111.01: "[T]he words of a claim must be given their plain meaning unless applicant has provided a clear definition in the specification." Applicant has provided a clear definition in the specification for the term "multiple-use unique identifier." Specifically, Applicant's specification states:

> Accordingly, appliance ID 210 is **referred to herein** as a multiple-use unique identifier since the appliance ID 210 uniquely identifies the appliance and identifies the appliance as an authorized device to embodiments of the private database wireless access system 100. (Emphasis added: see para. [28]: p. 6 last paragraph).

Nowhere does Garrison in view of Rezvani teach or suggest a multiple-use unique identifier that uniquely identifies both the appliance and the appliance as an authorized device.

The Examiner argues that the claimed multiple-use unique identifier is taught in Rezvani at paragraphs [0004] and [0006]. Applicant strongly disagrees. Paragraph [0004] in Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Paragraph [0006] states wireless devices used to track inmates "transmit a packet of information at a designated time interval in order to note the existence of the inmate." Importantly, notice that nowhere does Rezvani teach or suggest whatsoever that the ESN itself is used to identify the wireless device and provide access to a private database. In other words, Revzani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggest that the ESNs are "included in all transmitted RF communications from the wireless device" so the wireless device can

access a remote private database when the ESN "corresponds to a security indicia residing in the database device" as recited in claim 19.

For at least these reasons, claims 19, 22, 24, and 25 and their dependent claims are allowable over Garrison in view of Rezvani and Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki.

Third, claim 19 recites that the processor transmits a first RF communication to the database device that has both (1) the appliance ID and (2) the private database access request. Nowhere does Garrison in view of Rezvani teach or suggest that a first RF communication includes both an appliance identification and a private database access request.

The Office Action has not provided locations in Garrison and Rezvani that teach or suggest RF communications to database, wherein the RF communications have both (1) the appliance ID and (2) the private database access request. Such teachings or suggestions do not exist in the art of record.

For at least these reasons, claims 19, 22, 24, and 25 and their dependent claims are allowable over Garrison in view of Rezvani and Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki.

Independent claim 27

Claim 27 recites that a portable wireless communication device (PWCD) provides an access request to a private database. The access request includes (1) an identification of the remote database and (2) an identification of the PWCD. Nowhere does Garrison teach or suggest that the **access request itself** includes identification of the PWCD. By contrast, Garrison teaches that the user or client transmits a password to identify himself (i.e., the user), not the appliance device. Garrison states:

> In accordance with another feature of the present invention, the client initially transmits a password to the server in order **to identify the user** of the client as an authorized user. (Emphasis added: [0016]).

In other words, Garrison teaches that the user sends a password to identify himself as an authorized user. This teaching is in contrast to the claimed recitations. Claim 27 recites receiving the access request at a remote database. The access request includes both (1) an identification of the remote database and (2) an identification of the PWCD. The combination of Garrison and Rezvani does not teach this element.

Garrison repeatedly reiterates that his access request identifies the user, not the wireless device. FIG. 4A is a flow chart illustrating the method of Garrison. The client computer and server utilize a public key exchange to establish a new encryption key (see [0065]). Garrison then teaches how the access request is performed:

> After receiving the new encryption key from the server 17a, the client 14 encrypts the user's password and log name with the new encryption key and transmits the password and log name to the server 17a ….
>
> The server 17a compares the log name transmitted by the client 14 with the log name in the password data table entry corresponding with the password. If the log names match, the user of the client 14 is determined to be an authorized user. (See [0066 – 0067]: portions omitted for brevity).

Nowhere does this section or any section of Garrison teach or suggest that the access request includes an appliance identification. Instead, Garrison expressly teaches that the user sends a password and log name. A password and log name, however, do not include an appliance identification. Nowhere is the actual appliance identified in Garrison.

In paragraphs [0004], [0108-0111], and [0113], Rezvani teaches cellular phones have ESNs and that various communication links can be used to connect a wireless device with a server. Importantly, notice that nowhere does Rezvani teach or suggest whatsoever that the ESN itself is used to identify the wireless device and provide access to a remote database. In other words, Revzani teaches that ESNs on cellular phones are

known. But, Rezvani never teaches or suggest that the ESNs are transmitted with a request to access a remote database, the request including the ESN and an identification of the remote database. Further, Rezvani never teaches or suggests that the ESNs are received at a remote database and then verified as to whether the ESN is "valid for allowing the PWCD to have access to information stored in the remote database" as recited in claim 27.

For at least these reasons, claim 27 and its dependent claims are allowable over Garrison in view of Rezvani and Shimada, Wilber, Khouri, Obouchi, Ronen, or Yamazaki.

Garrison Teaches Away

Garrison actually teaches away from the recitations of claim 27.[2] In claim 27, the database receives an access request from the wireless device. The access request includes (1) the database access request and (2) the appliance ID. If the appliance ID is verified as being valid at the database, then the database allows access. In other words, access to the database depends on the appliance ID of the wireless device. Applicant's specification supports this "simplified, yet secure, access to a private database" ([16]):

> Accordingly, the user requesting private database access with the wireless communication device need not enter a special password or the like because the wireless communication device is recognized by the remote database device. (para. [16]).

By contrast, access to the database in Garrison depends on a complex encrypted password key exchange between a user and the server. Garrison expressly teaches that a user engages numerous steps exchanging various encrypted public keys, passwords, log names, etc. in order to ensure a secure communication between the client and server (see [0064-0067]).

[2] Garrison also teaches away from the combination of Rezvani which teaches automatically identifying the wireless communication device.

For at least these additional reasons, claim 27 and its dependent claims are allowable over Garrison in view of Rezvani.

Dependent Claim 14

Dependent claim 14 recites transmitting a phone number of the wireless communication device as the appliance ID.The Examiner argues that this recitation is taught in Rezvani at paragraphs [0004] and [0006]. Applicant strongly disagrees.

Paragraph [0004] in Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Paragraph [0006] states wireless devices used to track inmates "transmit a packet of information at a designated time interval in order to note the existence of the inmate." Importantly, notice that nowhere does Rezvani teach or suggest whatsoever that a phone number is used to identify the wireless device and provide access to a private database. In other words, Revzani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggest that phone numbers are transmitted as an appliance ID to authorize access to a private database.

Dependent Claim 15

Dependent claim 15 recites "accessing the private database based on identification and authorization of the wireless communication device, **not identification of a user of the wireless communication device**" (emphasis added). Garrison and Rezvani do not teach or suggest these recitations.

Garrison disloses a complex encrypted password key exchange between a user and the server. Garrison expressly teaches that a user engages numerous steps exchanging various encrypted public keys, passwords, log names, etc. in order to identify the user (see [0064-0067]). Garrison actually teaches away from the recitations of dependent claim 15.

Paragraph [0004] in Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Rezvani never discloses or suggests that an ESN is used to access a private database based on identification and

authorization of the wireless communication device, not identification of a user of the wireless communication device.

Dependent Claim 16

Dependent claim 15 recites "granting access to the private database **without requiring a user of the wireless communication device to enter a password**" (emphasis added). Garrison and Rezvani do not teach or suggest these recitations.

Garrison disloses a required complex encrypted password key exchange between a user and the server. Garrison expressly teaches that a user engages numerous steps exchanging various encrypted public keys, passwords, log names, etc. in order to identify the user (see [0064-0067]). Garrison actually teaches away from the recitations of dependent claim 16.

Paragraph [0004] in Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Rezvani never discloses or suggests that an ESN is used to access a private database without requiring a user of the device to enter a password.

Dependent Claim 28

Claim 28 recites transmitting, via both the internet and the RF communication, the information from the remote database to the PWCD. In other words, claim 28 recites two different forms of communication for transmitting information to the remote database. Garrison teaches internet communication but not RF communications. Thus, Garrison does not teach all the elements of claim 28.

The Examiner argues that since Garrison mentions cellular connections in paragraph [0033], claim 28 is obvious. Applicant disagrees. Garrison does state that the communication network 18 in FIG. 1 can be a cellular network. Garrison, though, never shows multiple networks (i.e., both RF compatible and internet compatible networks). Further, Garrison never suggests that such multiple networks could be used such that both internet and RF communications are used to transmit data to and from a wireless device and a private remote database. How would such multiple networks be configured?

Garrison never discusses such embodiments because his embodiments only show and suggest a single network 18.

Dependent Claims 30 and 31

Garrison in view of Rezvani do not teach or suggest the elements of claims 30 and 31. Claim 30 is selected for discussion.

Claim 30 recites that the PWCD is a cellular phone, and the ID is a cellular phone number of the cellular phone. In other words, claim 30 recites that a cellular phone number is transmitted to a remote database and used to grant access to the cellular phone to the database. Nowhere does Garrison in view of Rezvani teach or suggest that a cellular phone number is transmitted to a remote database and then verified to allow the cellular phone to have access to the database.

The Examiner argues that this element in taught in Rezvani's ESNs. Applicant strongly disagrees. Nowhere does Rezvani teach or suggest whatsoever that the ESN itself is used to identify the wireless device and provide access to a remote database. In other words, Revzani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggest that the ESNs are transmitted with a request to access a remote database, the request including the ESN and an identification of the remote database. Further, Rezvani never teaches or suggests that the ESNs are received at a remote database and then verified as to whether the ESN is "valid for allowing the PWCD to have access to information stored in the remote database."

III. Claim Rejections: 35 USC § 103(a)

Claim 32 is rejected under 35 USC § 103 as being unpatentable over Garrison and Rezvani and (Shimada or Wilber or Khouri or Obouchi or Ronen or Yamazaki) in further view of USPN 6,178,505 (Schneider). This rejection is traversed.

Claim 32

Claim 32 recites authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in the remote database. The art of record does not teach or suggest this element.

Garrison actually teaches away. Access to the database in Garrison depends on a complex encrypted password key exchange between a user and the server. Garrison expressly teaches that a user engages numerous steps exchanging various encrypted public keys, passwords, log names, etc. in order to ensure a secure communication between the client and server (see [0064-0067]). Claim 32, however, recites "without a user of the PWCD entering a password." Thus, the combination of Garrison with Schneider is not proper.

The Examiner cites Schneider at column 3, lines 16-27. This section teaches that firewalls have different degrees of trust depending on the source of information. Nowhere does Schneider teach or suggest the recitations as actually recited in claim 32. Claim 32 recites authenticating a wireless device without a user entering a password so the wireless device can access a remote database. Schneider is completely unrelated to the claim elements.

CONCLUSION

In view of the above, Applicant respectfully requests the Board of Appeals to reverse the Examiner's rejection of all pending claims.

Any inquiry regarding this Amendment and Response should be directed to Philip S. Lyren at Telephone No. (832) 236-5529. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

/Philip S. Lyren #40,709/

Philip S. Lyren
Reg. No. 40,709
Ph: 832-236-5529

VIII. Claims Appendix

1. A method for communicating information from a private database to a wireless communication device, the method comprising:

receiving a private database access request from the wireless communication device, the private database access request including at least an appliance identification (ID) that uniquely identifies the wireless communication device;

comparing the appliance ID with a security indicia, the security indicia associated with the wireless communication device; and

communicating the information from the private database to the wireless communication device when the appliance ID corresponds to the security indicia, wherein verification of only the appliance ID is sufficient to authorize access to the private database.

2. The method of claim 1, wherein the appliance ID is multiple-use identification indicia that is included in all communications from the wireless communication device.

3. The method of claim 2, wherein the multiple-use identification indicia and the security indicia correspond to a telephone number of the wireless communication device.

4. The method of claim 1, wherein the appliance ID is a unique identifier included in a header information of the private database access request from the received wireless communication device.

5. The method of claim 1, wherein communicating further comprises transmitting the information as a radio frequency (RF) signal to the wireless communication device.

6. The method of claim 1, wherein receiving the private database access request further comprises receiving information selecting one of a plurality of different private databases wherein the selected private database is communicated to the wireless communication device when the appliance ID corresponds to the security indicia.

7. The method of claim 1, further comprising;

receiving a second private database access request from a second wireless communication device, the second private database access request including at least a password generated by a user;

comparing the received password with a security code, the security code uniquely associated with the user; and

associating a second security indicia with a second unique appliance ID of the second wireless communication device when the received password corresponds to the security code, so that the private database is communicated to the second wireless communication device.

8. The method of claim 7, further comprising saving the second unique appliance ID as the second security indicia uniquely associated with the second wireless communication device.

9. The method of claim 7, further comprising:

receiving a subsequent private database access request from the second wireless communication device, the subsequent private database access request including at least the second unique appliance ID;

comparing the second unique appliance ID with the second security indicia; and

communicating the private database to the second wireless communication device when the second unique appliance ID corresponds to the second security indicia.

10. The method of claim 1, further comprising:

uniquely associating a plurality of unique appliance IDs with a plurality of unique security indicia, wherein one appliance ID uniquely identifies one of a plurality of wireless communication devices and wherein each of the security indicia are uniquely associated with one of a plurality of private databases;

receiving the private database access request from one of the plurality of wireless communication devices, the private database access request comprising at least the

appliance ID of the transmitting wireless communication device and an access request to a selected private database selected from the plurality of private databases;

comparing the appliance ID of the transmitting wireless communication device with the plurality of unique security indicia; and

communicating the selected private database to the transmitting wireless communication device when the appliance ID corresponds to the security indicia of the selected private database.

11. The method of claim 1, further comprising receiving a communication from the wireless communication device that prevents association of the appliance ID with the security indicia so that communicating the information from the private database to the wireless communication device is prevented.

12. A method for remotely accessing a private database residing in a remote database device using a wireless communication device, the method comprising:

transmitting a radio frequency (RF) communication to the remote database device, the RF communication comprising a private database access request and comprising an appliance identification (ID) that uniquely identifies the wireless communication device; and

verifying only the appliance ID in order to authorize the wireless communication device to access the private database.

13. The method of claim 12, further comprising communicating a multiple-use identification indicia corresponding to the appliance ID and that uniquely identifies the wireless communication device, and wherein the multiple-use identification indicia is included in all communications from the wireless communication device.

14. The method of claim 12, further comprising transmitting a phone number of the wireless communication device as the appliance ID.

15. The method of claim 12, further comprising accessing the private database based on identification and authorization of the wireless communication device, not identification of a user of the wireless communication device.

16. The method of claim 12, further comprising granting access to the private database without requiring a user of the wireless communication device to enter a password.

17. The method of claim 12, further comprising:

selecting a portion of the received private database using a browser; and

displaying the selected portion of the received private database on a display residing on the wireless communication device using the browser.

18. The method of claim 12, further comprising communicating an instruction to the remote database device that prevents association of the appliance ID with the security indicia so that communicating the private database to the wireless communication device is prevented.

19. A system that remotely accesses a private database using a wireless communication device, the wireless communication device comprising:

a transceiver configured to receive and transmit radio frequency (RF) communications;

an appliance identification (ID) corresponding to a multiple-use unique identifier of the wireless communication device that is included in all transmitted RF communications from the wireless communication device; and

a processor configured to cause the transceiver to transmit a first RF communication to a database device having at least one private database, the first RF communication comprising the appliance ID and a private database access request so that verification of only the appliance ID authorizes the wireless communication device to access information stored in the private database.

20. The system of claim 19, further comprising a memory configured to store information received from the private database.

21. The system of claim 19, further comprising:

a display; and

a browser configured to display information received from the private database on the display.

22. A system that provides accesses to a private database comprising:

a communication system interface configured to receive a private database access request and a multiple-use unique identifier (ID) generated by a remote wireless communication device and configured to transmit a private database to the remote wireless communication device;

a security indicia that corresponds to the multiple-use unique ID, the multiple-use unique ID being included in all communications from the wireless communication device and uniquely identifying the wireless communication device; and

a processor configured to compare the multiple-use unique ID to the security indicia, and further configured to cause communication of the private database to the remote wireless communication device when the multiple-use unique ID corresponds to the security indicia, wherein verification of only the multiple-use unique ID is sufficient to authorize access to the private database.

23. The system of claim 22, further comprising a security code corresponding to a user associated with the private database, so that when the received ID is not initially associated with the security indicia, a password provided by the user of the remote wireless communication device causes the multiple-use unique ID to be associated with the security indicia when the password corresponds to the security code.

24. A computer-readable medium having a program for remotely accessing remote private databases using a wireless communication device, the program comprising logic configured to:

cause a transceiver to transmit a first radio frequency (RF) communication comprising a private database access request and a multiple-use unique identifier that uniquely identifies the wireless communication device, the first RF communication directed to a remote database device wherein a private database resides, and wherein the multiple-use unique identifier is included in all RF communications from the wireless communication device; and

cause the transceiver to receive a second RF communication comprising at least the private database, the private database communicated to the wireless communication device by the remote database device when the multiple-use unique identifier corresponds to a security number residing in the remote database device, wherein verification of the multiple-use unique identification alone is sufficient to authorize access to the private database.

25. A method for communicating information from a private database to a wireless telephone, the method comprising:

transmitting a radio frequency (RF) communication from the wireless telephone to a remote database device wherein the private database resides, the RF communication comprising at least a private database access request and comprising an appliance identification (ID) that uniquely identifies the wireless telephone, the appliance ID being included in all communications from the wireless telephone and uniquely identifying the wireless telephone;

receiving the private database access request and the appliance ID by the remote database device;

comparing only the appliance ID with a security indicia to determine if the wireless telephone has authorization to access the private database, the security indicia associated with the wireless communication device;

communicating the information of the private database from the remote database device when the appliance ID corresponds to the security indicia; and

receiving a second RF communication by the wireless telephone comprising at least the information of the private database.

26. The method of claim 25 wherein the appliance ID is a telephone number.

27. A method of software execution for remotely accessing a remote database using a portable wireless communication device (PWCD), the method comprising:

transmitting, via a radio frequency (RF) communication, an access request from the PWCD to the remote database, the access request including an identification of the remote database and an identification (ID) of the PWCD;

receiving, via an internet, the access request at the remote database; and

verifying, at the remote database, only the ID to determine whether the PWCD has authority to access information stored in the remote database.

28. The method of claim 27 further comprising transmitting, via both the internet and the RF communication, the information from the remote database to the PWCD.

29. The method of claim 27 further comprising displaying, using a browser in the PWCD, information received from the remote database.

30. The method of claim 27 wherein the PWCD is a cellular phone, and the ID is a cellular phone number of the cellular phone.

31. The method of claim 27 further comprising recognizing, at the remote database, a cellular phone number in the access request for identifying the PWCD as authorized to access the information stored in the remote database.

32. The method of claim 27 further comprising authenticating, without a user of the PWCD entering a password, whether the PWCD is authorized to access the information stored in the remote database.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.